AO 106 (Rev. 04/10) Application for a Search Warrant

# UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

data associated with the Instagram profile with URL: https://www.instagram.com/lilmac_gs9/, and more fully described in attachment A

Case No. 19-981M(NJ)

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:
Title 18, United States Code, Section 1073

The application is based on these facts: See attached affidavit.

☒ Delayed notice of _____ days (give exact ending date if more than 30 days: May 25, ~~2019~~ 2020) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Jeremy Loesch, Supervisory Deputy
*Printed Name and Title*

Sworn to before me and signed in my presence:

Date: November 25, 2019

*Judge's signature*

City and State: Milwaukee, Wisconsin

Nancy Joseph, U.S. Magistrate Judge
*Printed Name and Title*

## AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Jeremy Loesch, being duly sworn, hereby depose and say:

1. I am currently employed as a Supervisory Deputy for the U.S. Marshals Service. I have been employed as a law enforcement officer for 16 years. As a part of my duties, I investigate violations of federal and state laws including those relating to fugitives.

2. This Affidavit is made in support of an application for a search warrant to search the Target Account, more fully described in Attachment A, for evidence, instrumentalities, and proceeds, more fully described in Attachment B, for violations Title 18, United States Code, Section 1073.

3. The facts set forth in this Affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement agents and witnesses. This Affidavit is intended to show that there is probable cause to believe that evidence, instrumentalities, and proceeds, more fully described in Attachment B, for the subject offenses listed above will be found in the subject accounts, more fully described in Attachment A, and does not purport to set forth all of my knowledge of or investigation into this matter.

## STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

4. Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

a. Title 18, United States Code, Section 2703(a) provides, in part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental

entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Title 18, United States Code, Section 2703(b) provides, in part:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant□.
>
> (2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computer service; and
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. The government may also obtain records and other information pertaining to a subscriber to or customer of electronic communication service or remote computing service by way of a search warrant. See 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. See 18 U.S.C. § 2703(c)(3).

d. The statute permits the warrant to be served on the provider, who will then disclose the relevant records to the officer, who need not be onsite at the time the search is executed. Title 18, United States Code, Section 2703(g), provides, in part:

Presence of Officer Not Required Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

e. Title 18, United States Code, Section 2711, provides, in part:

As used in this chapter

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

f. Title 18, United States Code, Section 2510, provides, in part:

(8) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

(14) "electronic communications system" means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; . . .

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications; . . .

(17) "electronic storage" means

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

## INSTAGRAM TECHNICAL BACKGROUND

5. From my review of publicly available information provided by Instagram about its service, including Instagram's "Privacy Policy," I am aware of the following about Instagram and about the information collected and retained by Instagram.

6. Facebook Inc. is the corporate entity that provides the Instagram service, which owns and operates a free-access social-networking website under the name Instagram that can be accessed at http://www.instagram.com. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application ("app") created by the company that allows users to access the service through a mobile device.

7. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various "tags" that can be used to search for the photo (e.g., a user may add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of "filters" or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also "like" photos.

8. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by Instagram.

9. Instagram asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user's full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram collects and maintains this information.

10. Instagram allows users to have "friends," which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Instagram collects and maintains this information.

11. Instagram also allows users to "follow" another user, which means that they receive updates about posts made by the other user. Users may also "unfollow" users, that is, stop following them or block the, which prevents the blocked user from following that user.

12. Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Instagram collects and maintains user content that users post to Instagram or share through Instagram.

13. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user's feed, search history, or profile.

14. Users on Instagram may also search Instagram for other users or particular types of photos or other content.

15. For each user, Instagram also collects and retains information, called "log file" information, every time a user requests access to Instagram, whether through a web page or through an app. Among the log file information that Instagram's servers automatically record is the particular web requests, any Internet Protocol ("IP) address associated with the request, type of browser used, any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.

16. Instagram also collects and maintains "cookies," which are small text files containing a string of numbers that are placed on a user's computer or mobile device and that allows Instagram to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user's interests.

17. Instagram also collects information on the particular devices used to access Instagram. In particular, Instagram may record "device identifiers," which includes data files and other information that may identify the particular electronic device that was used to access Instagram.

18. Instagram also collects other data associated with user content. For example, Instagram collects any "hashtags" associated with user content (i.e., keywords used), "geotags" that mark the location of a photo and which may include latitude and longitude information, comments on photos, and other information.

19. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.

20. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal

conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user's account activity, IP log, stored electronic communications, and other data retained by Instagram, can indicate who has used or controlled the Instagram account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was accessed or used. For example, as described herein, Instagram logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under investigation. Additionally, Instagram builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Instagram "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner's state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or

consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

21. Based on the information above, the computers of Instagram are likely to contain all the material described above with respect to the SUBJECT ACCOUNT, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

## PROBABLE CAUSE

22. On May 13, 2019, a criminal complaint was issued in Milwaukee County Circuit Court, case number 2019CF002053, charging Hayes with (1) one count of 1st Degree Recklessly Endangering Safety, contrary to Wis. Stat. § 941.30(1), with a modifier of Use of a Dangerous Weapon, in violation of Wis. Stat. § 939.63(1)(b), and (2) one count of 2nd Degree Recklessly Endangering Safety, contrary to Wis. Stat. § 941.30(2), with a modifier of Use of a Dangerous Weapon, in violation of Wis. Stat. § 939.63(1)(b). An arrest warrant (warrant number K00390) and authorization for nationwide extradition were issued the same day. A copy of the criminal complaint and the associated arrest warrant are attached to this affidavit as Exhibit A. The charge of 1st Degree Recklessly Endangering Safety is a class F felony punishable by a term of imprisonment not to exceed 12 years and 6 months. The charge of 2nd Degree Recklessly Endangering Safety is a class G felony punishable by a term of imprisonment not to exceed 10 years. The modifier charge of Use of a Dangerous Weapon may increase the term of imprisonment for each of the charges not to exceed 5 years.

23. The criminal complaint alleges that, on April 27, 2019, Milwaukee Police Officers responded to Saint Joseph's Hospital, XXXX W. Burleigh St. Milwaukee, WI, regarding a person who arrived at the hospital with a gunshot wound to the back. Officers spoke with the victim, identified as "VT," who stated that he was seated inside a vehicle at his mother's residence, XXXX N. 52nd. St. Milwaukee, WI. While seated in the vehicle, VT observed Hayes along with his (VT's) ex-girlfriend, identified as "MB," approach the vehicle. Hayes was armed with a black semi-automatic handgun and MB was armed with a golf club. Hayes reportedly yelled at VT to exit the vehicle to which he attempted to drive away. VT reported hearing 4-5 gunshots and shortly after realized that he had received a gunshot wound to his back. Officers reviewed "Ring Doorbell" video recovered from the area of the shooting, which corroborated the victims' statement. Officers recovered fourteen 9mm casings and four flattened bullets from the scene. While conducting a neighborhood canvas, officers observed a bullet hole in the second story of XXXX W. Mill Rd. Milwaukee, WI. The homeowner reported to the officers that he and his three children were home when the shooting occurred and that one of his children was in her bedroom when a bullet entered the home and struck a TV in the bedroom.

24. Following the shooting, the Milwaukee Police Department's Fugitive Apprehension Unit made multiple endeavors to attempt to locate and arrest Hayes at several known family member's homes located in Milwaukee, WI. All efforts were met with negative results.

25. On July 10, 2019, the U.S. Marshals Fugitive Task Force was requested to assist in locating and arresting Hayes. The Milwaukee Police Department reported that they believed that Hayes had fled Wisconsin and may be in Miami, Florida based upon posts made by Hayes to his Facebook.com and Instagram.com pages.

26. On July 12, 2019, Deputy U.S. Marshal (DUSM) Bressers was assigned the fugitive investigation for Hayes.

27. On July 17, 2019, DUSM Bressers conducted an open records search of social media website Facebook.com. DUSM Bressers located a Facebook page under the name Demarcus Hayes with a URL and User ID Number of,

URL: https://www.facebook.com/lilxhayes
User ID Number: 100000494492986

DUSM Bressers reported observing several publicly posted photos of a male on this Facebook page. DUSM Bressers compared the Facebook photos to Hayes' Wisconsin Department of Transportation photo and found them to be the same person. A public posts made by Hayes on his Facebook.com page on July 11, 2019, "FOLLOW ME ON IG @LILMAC_GS9," directed viewers to "follow" him on his Instagram.com page. DUSM Bressers conducted an open records search of Instagram.com utilizing "lilmac_gs9" as a search term and located Hayes Instagram page. DUSM Bressers noted observing the same photos of Hayes that were posted to his Facebook.com page also being posted to Hayes' Instagram.com page. DUSM Bressers identified the URL for Hayes' Instagram.com page as **https://www.instagram.com/lilmac_gs9/**.

28. On, July 18, 2019, a search warrant for Hayes' Facebook.com account was signed by the Honorable Glenn H. Yamahiro, Milwaukee County Circuit Court Judge for records and content of the account.

29. On July 29, 2019, a search warrant for Hayes' Instagram.com account was signed by the Honorable David Swanson, Milwaukee County Circuit Court Judge for records and content of the account.

30. On August 14, 2019, a collateral lead (request for assistance) was sent to the Western District of Texas (W/TX) based upon information developed that Hayes was believed to

have fled to San Antonio, TX. Investigators with the Lone Star Fugitive Task Force in W/TX conducted an investigation into the whereabouts of Hayes.

31. On August 20, 2019, W/TX reported that Hayes had been residing in San Antonio with MB at XXXXX Huebner Rd. #2407 San Antonio, TX. The managers of the apartment complex identified Hayes from a known picture and identified Hayes as MB's boyfriend. The managers reported that Hayes was no longer residing with MB and moved to New York.

32. Information received from Facebook.com identified a private message conversation between Hayes and screen name "TrapStan SevenFoe." A portion of the conversation occurring from May 5, 2009 from 22:33:17 to 22:35:15 is as follows,

TrapStan SevenFoe: "That wat up"

Demarcus Hayes: "Dude bitch ass really told"

TrapStan SevenFoe: "Smh u still in town or left"

Demarcus Hayes: "I'm in cali"

TrapStan SevenFoe" "Wit tee"

Demarcus Hayes: "Nah we link up next week in New York"

TrapStan SevenFoe: "Aww ok"

33. Information received from Facebook.com identified a private message conversation between Hayes and screen name "Briggs Alexis." On May 14, 2019 at 14:08:01 Hayes posted,

"Cuzin im literally on the run for attempted murder and this bitch took all da money n left me in madison g this hotel finna make me checkout at 11 and ian got not car or no cheese ima literally be outside cuz can u please look out for me I'll pay u back g"

34. On September 30, 2019, a collateral lead was sent to the U.S. Marshals New York/New Jersey Regional Fugitive Task Force (NY/NJRFTF) requesting assistance in locating and arresting Hayes. As of November 22, 2019, NY/NJRFTF Investigators have been unable to locate and arrest Hayes.

35. Hayes regularly posts publicly on his Facebook and Instagram pages.

36. Hayes last posted on Facebook on November 19, 2019 at 9:14 a.m. Accordingly, I believe that Hayes continues to use his Facebook account while attempting to avoid prosecution in Wisconsin state court.

37. Hayes was last active on Instagram on November 21, 2019. Accordingly, I believe that Hayes continues to use his Instagram account while attempting to avoid prosecution in Wisconsin state court.

38. Since April 27, 2019, Hayes has avoided apprehension and remains at large, despite the Milwaukee Police Department's Fugitive Apprehension Unit and United States Marshals Service's Fugitive Task Force's attempts to locate and arrest him.

39. On November 21, 2019, a criminal complaint and arrest warrant were issued by the Honorable Magistrate Judge Nancy Joseph charging Hayes with a single count of Unlawful Flight to Avoid Prosecution in violation of Title 18, United States Code, Section 1073.

40. Based on your affiant's training and experience in locating and apprehending potentially violent fugitives, the data being sought by this warrant will assist in locating Hayes. Because successful apprehensions, particularly of violent fugitives, often rely on the element of surprise and on taking the fugitive by unaware, it is often necessary to attempt an arrest during nighttime or the early morning hours, when most people are sleeping. Further, apprehension tactical plans often change at the last minute based on unexpected movements or other behavior

of the target. Therefore, I cannot predict in advance when this data would need to be accessed, and would need access to the data at all times of the day or night in order to ensure a safe and successful apprehension.

## CONCLUSION

41. Based on the facts set forth in this Affidavit, your Affiant submits that there is probable cause to believe that the subject accounts contain the fruits, instrumentalities, and evidence of the subject offenses.

## ATTACHMENT A

This Search Warrant is being sought for the data specified in Attachment B associated with the following Instagram profile with URL:

https://www.instagram.com/lilmac_gs9/

hosted by Facebook Inc., 1601 Willow Road, Menlo Park, California, USA.

## ATTACHMENT B

### I. Information to be disclosed by Instagram, whose parent company is Facebook Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, the Provider is required to disclose the following information to the government for each account listed in Attachment A:

(a) All physical location data collected by the Provider for the user of the account, including any data collected by the Provider's location services via the user's mobile phone or other device, on a real-time or near-real time basis. The Provider is required to provide any such data they collect, regardless of the time of day.

### II. Information to be seized by the government

(a) All data disclosed by the Provider pursuant to this attachment. This data shall be made accessible by the provider to the United States Marshals Service 24/7, day or night, and/or emailed to Supervisory Deputy United States Marshal Jeremy Loesch at jeremy.loesch@usdoj.gov.

### III. Time for production by provider

The provider shall begin producing the information required by this attachment within seven (7) days of the date of service of the warrant.

## IV. Duration of production

The provider shall produce the information required by this attachment for a period of sixty (60) days from the date of issuance of this warrant.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Instagram, LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Instagram, LLC. The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Instagram, LLC, and they were made by Instagram, LLC as a regular practice; and

b. such records were generated by Instagram, LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Instagram, LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Instagram, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

| | |
|---|---|
| Date | Signature |